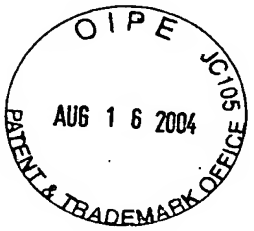
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Joachim Schmidt
Serial No.:	10/825,583
For:	Process and Device for the Packet Oriented Transmission of Security- Relevent Data
Filed:	August 15, 2004
Examiner:	Not Yet Assigned
Art Unit:	2131
Attorney Docket:	2133.034USU
Confirmation No.:	8182
Customer No.:	27,623



Mail Stop Missing Parts
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR ENTRY OF PRIORITY CLAIM AND SUBMISSION OF PRIORITY DOCUMENT

Dear Sir:

Applicant hereby requests that a priority claim under 35 U.S.C. §119 be entered in the above-identified application as follows: German Application No. 103 18 068.0 filed April 17, 2003, for the above noted application.

We are also enclosing a certified copy of the priority document, German Application No. 103 18 068.0 filed 17 April 2003, for filing in the above noted application.

It is respectfully requested that this application be passed to allowance.

Respectfully submitted,

Date: August 13,2004

Charles N.J. Ruggiero, Esq.
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
Attorney for Applicants
Registration No. 28,468
One Landmark Square, 10th Floor
Stamford, Connecticut 06901-2682
Telephone: (203) 327-4500
Telefax: (203) 327-6401

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	103 18 068.0
Anmeldetag:	17. April 2003
Anmelder/Inhaber:	Phoenix Contact GmbH & Co KG, 32825 Blomberg/DE
Bezeichnung:	Verfahren und Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten
IPC:	H 04 L 12/56

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 22. April 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

CERTIFIED COPY OF
PRIORITY DOCUMENT

A 9161
06/00
EDV-L

Phoenix Contact GmbH &Co

Verfahren und Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten

Beschreibung

Die Erfindung betrifft ein Verfahren und Vorrichtungen zum Paket-orientierten Übertragen sicherheitsrelevanter Daten.

Insbesondere bei der Übertragung sicherheitsrelevanter Daten über ein ungesichertes Medium, wie beispielsweise über ein herkömmliches Netzwerk und/oder Bussystem, wird solchen Daten in der Regel eine hochwertige Redundanz hinzugefügt, so dass nahezu alle statistischen und systematischen Fehler des gesamten Übertragungssystems keine negative Auswirkung auf die Integrität der Daten haben und hohen sicherheitstechnischen Anforderungen im Hinblick auf die Kommunikation zwischen einzelnen Netz- und/oder Busteilnehmern entsprochen wird.

Üblicherweise geschieht dies durch die Erweiterung der sicherheitsrelevanten Daten um einen Datensicherungswert, welcher basierend auf den sicherheitsrelevanten Daten generiert und dem jeweiligen Protokoll entsprechend, den sicherheitsrelevanten Daten eines zu übertragenden Datenpakets angehängt wird.

Aus der Deutschen Offenlegungsschrift DE 100 65 907 A1 ist beispielsweise ein Verfahren offenbart, welches auf dem allgemein bekannten Prinzip einer "Redundanz mit

Kreuzvergleich" beruht. Hierbei werden senderseitig, je nach Art der Applikation einkanalig oder zweikanalig zur Verfügung gestellte sicherheitsrelevante Daten zweifach, d.h. in zwei Datenpaketen, und unabhängig voneinander mit redundanter Information aufbereitet und über separate Verbindungen oder zeitlich nacheinander über eine Verbindung zur Empfangsseite übertragen. Je nach Applikation kann der Dateninhalt eines der beiden aufbereiteten sicherheitsgerichteten Datenpakete auch invertierte Daten oder andere zusätzliche Verschachtelungen aufweisen, um beispielsweise auch systematische Fehler in den Sendern, Empfängern und/oder anderen die Daten weiterleitenden Einheiten zu erkennen. Darüber hinaus ist gemäß Offenbarung vorgesehen, senderseitig und/oder empfängerseitig die beiden aufbereiteten Datenpakete kreuzweise auf Richtigkeit zu überprüfen, indem die innerhalb der Datenpakete jeweils zugefügte Redundanz untersucht wird.

Die komplette sicherheitsgerichtete Nachricht nach dem Stand der Technik ist dann beispielsweise gemäß der beigefügten Figur 3 aufgebaut, wobei diese sicherheitsgerichtete Nachricht folglich zwei Datenpakete 3 und 3´ umfasst. Gemäß Fig. 3 enthalten die sicherheitsrelevanten Daten neben den eigentlichen Nutzdaten ferner zusätzliche Kontrolldaten, wobei jedes der Datenpakte 3 und 3´ diese Daten mit dem gleichen Informationsgehalt, jedoch unterschiedlich kodiert umfasst. Darüber hinaus enthält jedes Datenpaket 3 bzw. 3´ einen basierend auf den sicherheitsrelevanten Daten generierten Block redundanter Information CRC bzw. $\overline{CRC}$.

Ein wesentlicher Nachteil dieses an sich bekannten Verfahrens gemäß dem Stand der Technik liegt jedoch insbesondere in dem schlechten Verhältnis von Nutzdatenlänge zur Gesamtdatenlänge, welches sich bei abnehmender Anzahl von zu übertragenden Nutzdaten je Datenpaket, wie dieses

beispielsweise beim Interbus gegeben ist, zunehmend verschlechtert.

Eine Aufgabe der Erfindung besteht somit darin, einen neuen und gegenüber vorstehend aufgezeigtem Stand der Technik verbesserten Weg zur Paket-orientierten Übertragung sicherheitsrelevanter Daten bereitzustellen, mit welchen auch bei Gewährleistung einer wesentlich verbesserten Nutzdatenrate eine hochwertige Absicherung gegen statistische und systematische Fehler bei einem ungesicherten Übertragungsmedium sichergestellt ist.

Die erfindungsgemäße Lösung der Aufgabe ist auf höchst überraschende Weise bereits durch ein Verfahren mit den Merkmalen des Anspruchs 1, durch eine Vorrichtung mit den Merkmalen des Anspruchs 10 und durch ein Übertragungssystem mit den Merkmalen des Anspruchs 19 gegeben.

Vorteilhafte und/oder bevorzugte Ausführungsformen bzw. Weiterbildungen sind Gegenstand der jeweiligen abhängigen Ansprüche.

Erfindungsgemäß ist somit zum Paket-orientierten Übertragen sicherheitsrelevanter Daten, insbesondere unter Verwendung wenigstens eines Übertragungssystems, welches ein paralleles und/oder serielles Netzwerk und/oder Bussystem mit zumindest einem daran angeschlossenen Teilnehmer umfasst, vorgesehen, dass die sicherheitsrelevanten Daten und eine auf den sicherheitsrelevanten Daten basierende redundante Information in verschiedenen Paketen übertragen werden.

Folglich ist von wesentlichem Vorteil, dass eine hochwertige Absicherung gegen statistische und systematische Fehler, insbesondere im Fall einer Übertragung über ein ungesichertes Medium, bei einer wesentlich verbesserten Nutzdatenrate

gewährleistbar ist.

Zweckmäßiger Weise sieht die Erfindung somit die Bereitstellung einer Vorrichtung zum Paket-orientierten Übertragen sicherheitsrelevanter Daten zwischen wenigstens zwei Netzwerk- und/oder Busteilnehmern vor, die senderseitig angeordnete Mittel zum Paket-orientierten Einbetten von sicherheitsrelevanten Daten und zugeordneter redundanter Information in verschiedene Pakete aufweist und/oder empfangsseitig angeordnete Mittel aufweist, die zum Überprüfen einer fehlerfreien Übertragung sicherheitsrelevanter Daten basierend auf in unterschiedlichen Paketen eingebetteten sicherheitsrelevanten Daten und zugeordneter redundanter Information ausgebildet sind.

Die Erfindung ermöglicht somit darüber hinaus, dass lediglich Mittel zum Generieren, Übertragen und Überprüfen einer einzigen redundanten Informationseinheit zu jeder sicherheitsrelevanten Dateneinheit erforderlich sind, welches zu einer wesentlichen Vereinfachung bei der Datenverarbeitung, insbesondere von sicherheitsbasierten Eingangs- und/oder Ausgangseinrichtungen bzw. -teilnehmern eines Übertragungsnetzwerkes und/oder -busses führt.

Um zu gewährleisten, dass im Wesentlichen alle statistischen und systematischen Fehler im Übertragungssystem erkannt werden, ist in vorteilhafter eine Kodiereinrichtung vorgesehen, mit welcher die redundante Information entsprechend kodierbar ist.

In besonders bevorzugter Weiterbildung schlägt die Erfindung vor, für die redundante Information einen Datensicherungswert einzusetzen, der eine über den sicherheitsrelevanten Daten berechnete Checksumme enthält.

Eine derartige Checksumme ist hierbei beispielsweise unter Verwendung eines Polynoms derart wählbar, dass in besonders bevorzugter Weise jede der möglichen Checksummen aus genau einer der möglichen Kombinationen der sicherheitsrelevanten Daten hervorgeht.

Die Erfindung gewährleistet somit eine äußerst gute Absicherung gegen Bündelfehler sowie gegen Vertauschungen einzelner Komponenten der zu übertragenden sicherheitsgerichteten Nachricht insgesamt.

Gemäß praktischer Weiterbildung sind den senderseitig angeordneten Mitteln zum Einbetten treiberartige Mittel zum Generieren von redundanter Information zugeordnet, die die gleiche Anzahl von Bits aufweist wie sie die zu übertragenden sicherheitsrelevanten Daten aufweisen. Die Erfindung kann somit im Wesentlichen Applikations-spezifisch bei im Wesentlichen allen derzeit bekannten Netzwerken und/oder Bussystemen, wie beispielsweise dem Interbus, Ethernet, Profibus oder CAN eingesetzt werden.

Bei der erfindungsgemäßen Übertragung von sicherheitsrelevanten Daten und zugeordneter Redundanz in getrennten Paketen ist somit eine hohe Hammingdistanz einstellbar.

Da durch die Erfindung folglich ferner selbst bei einer geringen Anzahl von Nutzdaten eine hohe Dynamik bereits aufgrund nur eines sich ändernden Bits sichergestellt werden kann, ist bei der Weiterleitung der Daten eine besonders gute Erkennung auch von systematischen Fehlern insbesondere von nicht sicheren Netzwerk- und/oder Busteilnehmern, einschließlich Switches, Router, Verstärker, Gateways, Systemkoppler und/oder einem Master, gewährleistbar.

Die Erfindung sieht ferner je nach anwendungsspezifisch eingesetzten seriellen und/oder parallelen Netzwerken und/oder Bussystemen vor, dass die sicherheitsrelevanten Daten neben den eigentlichen Nutzdaten, also insbesondere Ein-/Ausgangsdaten und/oder andere sichere Prozessdaten weitere Daten, insbesondere Kontroll- und/oder Steuerdaten umfassen.

Ferner ist vorgesehen, die Pakete mit den einander zugeordneten sicherheitsrelevanten Daten und redundanten Informationen parallel oder seriell zu übertragen und/oder mehrere Pakete innerhalb eines vordefinierten (Über-)Rahmens zu übertragen, so dass die Erfindung bei unterschiedlichsten Applikationen und/oder Anwendungsgebieten einsetzbar ist. Insbesondere im letztgenannten Fall ist ferner bevorzugt vorgeschlagen, innerhalb der vordefinierten Struktur eines (Über-)Rahmens sicherheitsrelevante Daten und die darauf basierend generierte zugeordnete redundante Informationen gemeinsam zu übertragen, um die Implementierung für das empfangsseitige Bereitstellen von Mitteln zum Auslesen und Überprüfen der sicherheitsrelevanten Daten und zugeordneten redundanten Information insbesondere in Hinblick auf die Zuordnungfunktionalität zu vereinfachen.

Wenn die Pakete mit einander zugeordneten sicherheitsrelevanten Daten und redundanter Information voneinander getrennt übertragen werden, ist daher ferner in bevorzugter Weiterbildung vorgesehen, dass die zu übertragenden Datenpakete einen Adressierungsblock und/oder eine Kennung zur logischen Zuordnung umfassen. Eine derartige Adressierung und/oder Kennung wird in praktischer Ausführung von Applikations-spezifisch entsprechend angepassten senderseitigen Mitteln basierend auf dem jeweils eingesetzten Übertragungsformat in den zu übertragenden Datenpaketen

derart eingebettet und von entsprechend empfangsseitig ausgebildeten Auslesungsmitteln für eine logische Zuordnung von Datenpaketen mit einander zugeordneten Inhalten zur Überprüfung einer fehlerfreien Übertragung verifiziert.

Je nach Applikationsgebiet der Erfindung, welches beispielsweise in der Gebäudeleittechnik, der Prozessindustrie, der Fertigungsindustrie, beim Personentransport und/oder für den Betrieb einer Automatisierungsanlage liegt, sowie basierend auf der individuellen Struktur des jeweiligen Netzwerks und/oder Bussystems, welches insbesondere eine ring-, linien-, stern- und/oder baumförmig ausgebildeten Struktur aufweist, ermöglicht die Erfindung in vorteilhafter Weise die Integration der vorstehend aufgeführten senderseitigen und empfangseitigen erfindungsgemäßen Mittel im Wesentlichen in jeder Teilnehmereinrichtung, also insbesondere in Master- und/oder Slaveteilnehmer.

Die Erfindung wird nachfolgend anhand eines bevorzugten Ausführungsbeispiels unter Bezugnahme auf die beigefügten Zeichnungen beschrieben.

In den Zeichnungen zeigen:

Fig. 1 einen erfindungsgemäßen Aufbau von Datenpaketen zum Paket-orientierten Übertragen sicherheitsrelevanter Daten,

Fig. 2 ein weiterer erfindungsgemäßer Aufbau zur Veranschaulichung der wesentlich verbesserten Erkennung von systematischen Fehlern, und

Fig. 3 der Aufbau einer sicherheitsgerichteten Nachricht nach dem Stand der Technik.

Bezug nehmend auf Fig. 1 ist zur Bereitstellung einer Paket-orientierten Übertragung sicherheitsrelevanter Daten unter

Gewährleistung einer hohen Nutzdatenrate bei gleichzeitiger hochwertiger Absicherung gegen statistische und systematische Fehler beispielhaft eine erfindungsgemäß zu übertragende sicherheitsgerichtete Nachricht dargestellt, welche zwei Datenpakete 1 und 2 umfasst.

Erfindungsgemäß weist eine sicherheitsgerichtete Nachricht eines sicherheitsrelevanten Satzes von Daten, wie bei Fig. 1 dargestellt, grundsätzlich wenigstens zwei separate Datenpakete 1 und 2 auf, von denen ein Datenpaket 1 sicherheitsrelevante Daten und ein weiteres Datenpaket 2 zugeordnete redundante Information umfasst.

Basierend auf diesem erfindungsgemäßen Aufbau ist sichergestellt, dass bei der Übertragung sicherheitsrelevanter Daten auch über ein ungesichertes Medium, also im Wesentlichen über ein Bus- und/oder Netzwerksystem, welches sicherheitsgerichteten Normen nicht genügt und/oder nicht sichere Systemteilnehmer umfasst, im Wesentlichen alle statistischen Fehler und systematischen Fehler erkennbar sind.

Statistische Fehler bei einer Datenübertragung basieren hierbei insbesondere auf von außen einwirkenden Störungen und/oder elektrischen Einflüssen, wohingegen systematische Fehler, herkömmlicherweise ihre Ursachen in Software- und/oder Hardware-basierten Fehlern von im Übertragungsweg angeordneten Sendern, Empfängern und/oder anderen, die Daten weiterleitenden Einrichtungen finden, wie beispielsweise Switches, Router, Verstärker, Gateways und/oder Systemkoppler.

Negative Auswirkungen derartiger Ursachen auf die Integrität sicherheitsrelevanter Daten sind folglich, wie nachfolgend näher beschrieben, im Wesentlichen vollständig ausschließbar.

Das bei Fig. 1 dargestellte Datenpaket 1 umfasst als sicherheitsrelevante Daten einen Protokoll– und/oder Applikations-spezifischen Nutzdatenblock 11 und im vorliegenden Beispiel einen Kontrolldatenblock 12.

Applikations-spezifisch werden derartige Nutzdaten 11 senderseitig, insbesondere von Sensoren, Aktoren und/oder Steuerungseinrichtungen ein- oder zweikanalig bereitgestellt und basierend auf der Gesamtstruktur des Übertragungssystems, welches ring-, linien-, stern- und/oder baumförmige Netz- und/oder Busstrukturen aufweisen kann, an eine definierte Empfangsseite, beispielsweise an einen Aktor oder Stell-Antrieb eines Schutzgitters übertragen. Solche Nutzdaten 11 umfassen folglich häufig reine Eingangs-/Ausgangsdaten. Einsatzgebiete von Übertragungssystemen, bei denen derartige Nutzdaten 11 teilweise oder vollumfänglich sicherheitsrelevante Daten darstellen, finden sich folglich insbesondere im Bereich der Fertigungsindustrie, des Personentransports, der Feuerungstechnik, der Prozessindustrie oder im Bereich der Gebäudeleittechnik.

Kontrolldaten 12 und/oder zusätzliche sichere oder nicht sichere Daten, wie beispielsweise Steuerdaten, oder wie bei Fig. 2 dargestellt, eine laufende Nummer 12b werden häufig zusätzlich zu diesen reinen Eingangs-/Ausgangsdaten 11 zur Prozesssteuerung generiert. Diese zusätzlichen Daten gestatten es beispielsweise den Kommunikationsteilnehmern im Wesentlichen die einwandfreie Funktion eines Gegenteilnehmers zu überprüfen, insbesondere durch Kontrolle des Übertragungspfades über Schrittketten durch jeweiligen Austausch von Kontrolldatenblöcken 12.

Das die sicherheitsgerichtete Nachricht vervollständigende Datenpaket 2 umfasst eine dem Informationsinhalt des

Datenpakets 1 zugeordnete redundante Information 21, also einen auf den Nutzdaten 11 und den Kontrolldaten 12 basierten Datensicherungswert 21.

Der in dem Datenpaket 2 enthaltene Datensicherungswert 21 ist zweckmäßigerweise eine über die Nutzdaten 11 und den Kontrollblock 12 berechnete Checksumme CRC, die senderseitig mit angepassten treiberartigen Mitteln, insbesondere einem Mikroprozessor oder einer ähnlichen programmierbaren Schaltungsanordnung, anhand eines Fehler-Prüf-Algorithmus, beispielsweise in Form eines an sich bekannten "Cycle Redundancy Check" generiert wird.

An der Empfangsseite oder einer definierten Weiterverarbeitungsstelle werden die Teilnachrichten 1 und 2 von Apllikations-spezifisch angeordneten, insbesondere Slave-Teilnehmern und/oder einem Master-Teilnehmer ausgelesen und durch Untersuchung der redundanten Information 21 in Bezug auf die sicherheitsrelevanten Daten 11 und 12 hinsichtlich einer fehlerfreien Übertragung überprüft, bevor die sicherheitsrelevanten Nutzdaten 11 an die entsprechenden Ausgangsteilnehmer, wie beispielsweise einem Aktor zu dessen Ansteuerung weitergereicht werden.

Da zu übertragende Datenpakete Protokoll-spezifisch grundsätzlich stets die gleiche Anzahl von Bits aufweisen, besitzen somit, wie bei Fig. 1 zu sehen, auch das Datenpaket 1, welches die sicherheitsrelevanten Daten, also im vorliegenden Beispiel die Nutzdaten 11 und zusätzlich die Kontrolldaten 12 umfasst, und das die Checksumme 21 umfassende Datenpaket 2 jeweils die gleiche Bitlänge n.

Folglich ist die Nutzdatenrate, also das Verhältnis von Nutzdatenlänge zu Gesamtdatenlänge, einer erfindungsgemäß aufgebauten sicherheitsgerichteten Nachricht im Vergleich zu

einer sicherheitsgerichteten Nachricht, bei welcher, wie bei Fig. 3 dargestellt, jedes Datenpaket 3 und 3´ sowohl, wenn auch unterschiedlich codiert, die sicherheitsrelevanten Daten, also insbesondere die Nutzdaten, als auch einen auf den sicherheitsrelevanten Daten basierten Datensicherungswert umfasst, wesentlich höher.

Basierend auf der Einbettung der sicherheitsrelevanten Daten 11, 12 und der redundanten Information 21 in zwei verschiedene Datenpakete 1 bzw. 2 muss folglich lediglich die Generierung eines Datensicherungswertes 21 durchgeführt werden und ermöglicht die Erfindung somit die Einsparung eines Datensicherungswertes gegenüber der Übertragung sicherheitsrelevanter Daten gemäß dem Stand der Technik (Fig. 3).

Um zusätzlich zur verbesserten Nutzdatenrate, insbesondere auch bei Übertragung eines lediglich eine geringe Anzahl von Nutzdaten 11 umfassenden sicherheitsrelevanten Datensatzes, darüber hinaus eine hochwertige Fehlerabsicherung für ein Senden und/oder Weiterleiten von sicherheitsrelevanten Daten durch nicht sichere Slave-Teilnehmern und/oder einem nicht sicheren Master zu gewährleisten, ist jedoch der folglich in der Anzahl der Bits gesteigerte Datensicherungswert 21 besonders effektiv.

Bevorzugt wird hierzu der Datensicherungswert 21, also insbesondere das CRC-Polynom bzw. der zur Generierung einer Checksumme verwendete Fehler-Prüf-Algorithmus so gewählt, dass jeder der 2^n möglichen Datensicherungswerte aus genau einer der 2^n Kombinationen der sicherheitsrelevanten Daten hervorgeht. Beide Datenpakete 1 und 2 der sicherheitsgerichteten Nachricht enthalten somit im Wesentlichen die gleichen Informationen, sind jedoch unterschiedlich kodiert.

Für die praktische Anwendung wird somit bei geeigneter Generierung der redundanten Information 21 eine sehr hohe Hammingdistanz bereitgestellt sowie eine gute Absicherung gegen Bündelfehler, gegen Vertauschen einzelner Komponenten der Daten der sicherheitsgerichteten Nachricht und eine gute Erkennung von Fehlern, insbesondere auch von systematischen Fehlern durch die unterschiedlichen Teilnachrichten 1 und 2, wie nachfolgend unter Bezugnahme auf Fig. 2 im einzelnen beschrieben, gewährleistet.

Bezug nehmend auf Fig. 2, bei welcher eine sicherheitsgerichtete Nachricht aus zwei jeweils 24 Bit umfassenden Datenpaketen 1b und 2b aufgebaut ist, wird die besonders gute Erkennung von systematischen Fehlern basierend auf der Erfindung besonders deutlich. Das die sicherheitsrelevanten Daten umfassende Datenpaket 1b umfasst hierbei zwei Bereiche, einen 16-Bit zählenden Nutzdatenbereich 11b und einen 8-Bit zählenden Bereich 12b zur Übertragung einer laufenden Nummer.

Wenn sich beispielsweise die zu sichernden Prozess- oder Eingangs-/Ausgangsdaten, also die 16-Bit umfassenden Nutzdaten 11b nicht ändern, zählt beispielsweise während einer Anwendung nur die laufende Nummer im Datenbereich 12b' hoch. Ist das Prüfpolynom 21b geeignet gewählt, ändern sich folglich in der großen, 24-Bit umfassenden Checksumme 21b immer eine ganze Reihe von Bits auf unterschiedlichsten Positionen. Diese hohe Dynamik der Nachrichten erlaubt es somit, systematische Fehler in den die sicherheitsgerichteten Nachrichten weiterleitenden Einrichtungen auf besonders einfache Weise und bei Gewährleistung höchster Sicherheit aufzudecken.

Anwendungsspezifisch bzw. basierend auf dem jeweiligen Netzwerk und/oder Bus gewährleistet die Erfindung darüber hinaus, dass die beiden, eine sicherheitsgerichtete Nachricht bildenden Teilnachrichten 1 und 2 auch innerhalb einer vordefinierten (Über-)Rahmenstruktur zusammengefasst werden und gemeinsam übertragen werden.

Grundsätzlich sei jedoch darauf hingewiesen, dass die Übertragung der beiden einander zugeordneten Teilnachrichten 1 und 2 auch getrennt, beispielsweise über separate Verbindung oder zeitlich nacheinander über eine Verbindung erfolgen kann. Ferner gewährleistet die Erfindung, dass die einander zugeordneten Teilnachrichten 1 und 2 auch innerhalb verschiedener vordefinierter (Über-)Rahmenstrukturen eingebettet und übertragen werden können. Hierzu ist zweckmäßigerweise vorgesehen, die einzelnen Pakete mit einem Adressierungsblock und/oder einer Kennung zur logischen Zuordnung zu versehen, so dass das empfängerseitige Auslesen, Zuordnen und Überprüfen auf fehlerfreie Übertragung von empfangenen Daten im Wesentlichen auch unabhängig von der zeitlichen Übertragung und/oder der Art und Weise der Übertragung der einander zugeordneten Teilnachrichten 1 und 2 durchführbar ist.

Die Erfindung ermöglicht somit, sicherheitsrelevante Daten bei einer hohen Nutzdatenrate über im Wesentlichen beliebige unsichere Medien zu übertragen, ohne dass die geforderte Sicherheit verloren geht. Beispielhaft sei an dieser Stelle auf den Interbus als ein für die Anwendung der Erfindung bevorzugtes Übertragungsmedium hingewiesen, bei welchem sichere Daten mit einer geringen Anzahl von Nutzdaten von nicht sicheren Teilnehmern und/oder dem nicht sicheren Master gesendet und/oder weitergeleitet werden.

Patentansprüche

1. Verfahren zum Paket-orientierten Übertragen sicherheitsrelevanter Daten (11, 11b, 12, 12b), insbesondere unter Verwendung wenigstens eines Übertragungssystems, welches ein paralleles und/oder serielles Netzwerk und/oder Bussystem mit zumindest einem daran angeschlossenen Teilnehmer enthält, wobei zusätzlich zu den sicherheitsrelevanten Daten (11, 11b, 12, 12b) eine auf den Daten basierende redundante Information (21, 21b) übertragen wird, dadurch gekennzeichnet, dass die sicherheitsrelevanten Daten (11, 11b, 12, 12b) und die auf diesen Daten basierende redundante Information (21, 21b) in verschiedenen Paketen (1, 1b, 2, 2b) übertragen werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die redundante Information (21, 21b) kodiert wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die redundante Information (21, 21b) eine über die sicherheitsrelevanten Daten berechnete Checksumme (CRC) ist.

4. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass die sicherheitsrelevanten Daten Nutzdaten (11, 11b), Kontrolldaten (12, 12b) und/oder Steuerdaten umfassen.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass mehrere Pakete (1, 1b, 2, 2b) innerhalb einer vordefinierten (Über-)Rahmenstruktur übertragen werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass Pakete innerhalb einer vordefinierten (Über-)Rahmenstruktur einander zugeordnete sicherheitsrelevante Daten (11, 11b, 12, 12b) und redundante Information (21, 21b) umfassen.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Pakete (1, 1b, 2, 2b) mit einander zugeordneten sicherheitsrelevanten Daten (11, 11b, 12, 12b) und redundanter Information (21, 21b) parallel oder seriell übertragen werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Pakete (1, 1b, 2, 2b) mit einander zugeordneten sicherheitsrelevanten Daten und redundanter Information aneinander gereiht oder voneinander getrennt übertragen werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Pakete (1, 1b, 2, 2b) einen Adressierungsblock und/oder eine Kennung zur logischen Zuordnung umfassen.

10. Vorrichtung, insbesondere für ein Übertragungssystem mit wenigstens einem parallelen und/oder seriellen Netzwerk und/oder Bussystem, zum Paket-orientierten Übertragen sicherheitsrelevanter Daten (11, 11b, 12, 12b), umfassend senderseitig angeordnete Mittel zum Paket-orientierten Einbetten von sicherheitsrelevanten Daten (11, 11b, 12, 12b) und zugeordneter redundanten Information (21, 21b) in verschiedene Pakete (1, 1b, 2, 2b).

11. Vorrichtung nach Anspruch 10, gekennzeichnet durch

eine Kodiereinrichtung zum Kodieren der redundanten Information (21, 21b).

12. Vorrichtung nach Anspruch 10 oder 11, dadurch gekennzeichnet, dass den Mitteln zum Einbetten Mittel zum Generieren von redundanter Information (21, 21b) mit gleicher Anzahl von Bits (n) wie die zu übertragende sicherheitsrelevanten Daten (11, 11b, 12, 12b) zugeordnet sind.

13. Vorrichtung nach Anspruch 10, 11 oder 12, dadurch gekennzeichnet, dass die Mittel zum Generieren und/oder Einbetten derart ausgebildet ist, dass aus jeder möglichen Kombination von sicherheitsgerichteten Daten (11, 11b, 12, 12b) eines Pakets (1, 1b) genau eine der möglichen Kombinationen innerhalb des Pakets (2, 2b) mit zugeordneter redundanter Information (21, 21b) eindeutig hervorgeht.

14. Vorrichtung, insbesondere für ein Übertragungssystem mit wenigstens einem parallelen und/oder seriellen Netzwerk und/oder Bussystem, zum Paket-orientierten Übertragen sicherheitsrelevanter Daten (11, 11b, 12, 12b), insbesondere nach einem der Ansprüche 10 bis 13, gekennzeichnet durch empfangsseitig angeordnete Mittel zum Überprüfen einer fehlerfreien Datenübertragung basierend auf sicherheitsrelevanten Daten (11, 11b, 12, 12b) und zugeordneter redundanter Information (21, 21b), die in verschiedenen Paketen (1, 1b, 2, 2b) eingebettet sind.

15. Vorrichtung nach Anspruch 14, dadurch gekennzeichnet, dass den Mitteln zum Überprüfen Mittel zum Auslesen und Zuordnen von mit unterschiedlichen Paketen empfangenen sicherheitsrelevanten Daten (11, 11b, 12, 12b) und

zugeordneter redundanter Information (21, 21b) zugeordnet sind.

16. Vorrichtung nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, dass mehrere Pakete (1, 1b, 2, 2b) mit sicherheitsrelevanten Daten (11, 11b, 12, 12b) und/oder zugeordneter redundanter Information (21, 21b) innerhalb einer vordefinierten (Über-)Rahmenstruktur übertragbar sind.

17. Vorrichtung nach einem der Ansprüche 10 bis 16, gekennzeichnet durch Mittel zum Paket-orientierten Einbetten und Auslesen von Adressierungsblöcken und/oder Kennungen zur logischen Zuordnung von einzelnen Paketen (1, 1b, 2, 2b) und/oder deren Inhalten (11, 11b, 12, 12b, 21, 21b) untereinander.

18. Vorrichtung nach einem der Ansprüche 10 bis 17, dadurch gekennzeichnet, dass die Mittel Slave-Einrichtungen und/oder einer Master-Einrichtung zugeordnet sind.

19. Übertragungssystem mit wenigstens einem parallelen und/oder seriellen Netzwerk und/oder Bussystem und mit wenigstens einer Vorrichtung nach einem der Ansprüche 10 bis 18.

20. Übertragungssystem nach Anspruch 19, welches wenigstens eine ring-, linien-, stern- und/oder baumförmig ausgebildete Netz- und/oder Bus-Struktur aufweist.

21. Übertragungssystem nach Anspruch 19 oder 20, umfassend wenigstens einen Interbus, ein Ethernet, einen Profibus und/oder ein CAN.

22. Verwendung eines Übertragungssystems nach Anspruch 19, 20

oder 21 in der Gebäudeleittechnik, Prozessindustrie, Fertigungsindustrie, zum Personentransport und/oder zum Betreiben einer Automatisierungsanlage.

Zusammenfassung

Die Erfindung betrifft das Paket-orientierte Übertragen sicherheitsrelevanter Daten.

Eine Aufgabe der Erfindung besteht darin, einen Weg zur Paket-orientierten Übertragung sicherheitsrelevanter Daten bereitzustellen, mit welchen bei Gewährleistung einer wesentlich verbesserten Nutzdatenrate eine hochwertige Absicherung gegen statistische und systematische Fehler bei einem ungesicherten Übertragungsmedium sichergestellt ist.

Die Erfindung schlägt, insbesondere unter Verwendung wenigstens eines parallelen und/oder seriellen Netzwerks und/oder Bussystems, ein Verfahren und Vorrichtungen zum Paket-orientierten Übertragen sicherheitsrelevanter Daten (11, 11b, 12, 12b) vor, bei welchen sicherheitsrelevante Daten (11, 11b, 12, 12b) und eine auf den Daten basierende redundante Information (21, 21b) in verschiedenen Paketen (1, 1b, 2, 2b) übertragen werden.

Fig. 1

Fig. 1

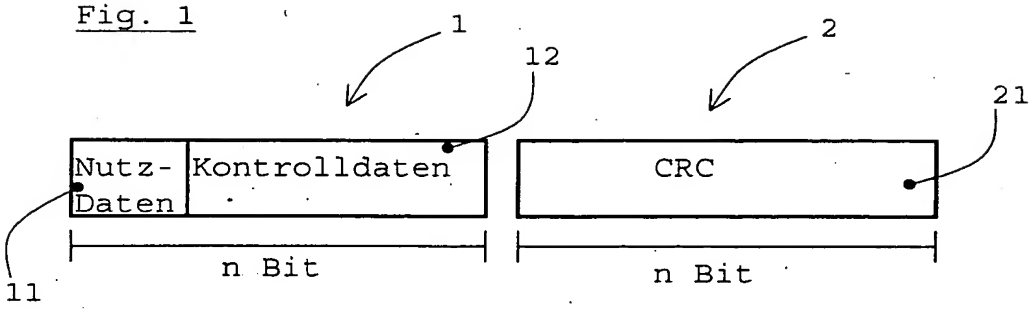


Fig. 2

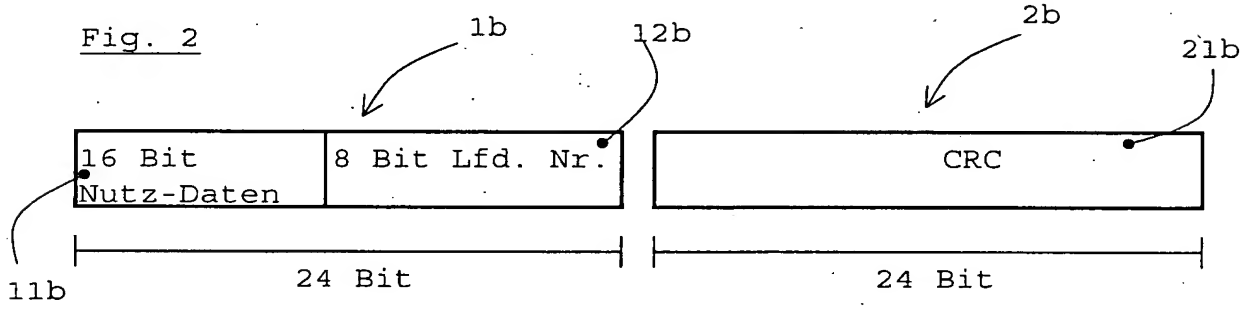


Fig. 3